The new EU cybersecurity framework

Markopoulou, Dimitra; Papakonstantinou, Vagelis; de Hert, Paul

Published in:
Computer Law and Security Review

DOI:
10.1016/j.clsr.2019.06.007

Publication date:
2019

Document Version
Version created as part of publication process; publisher's layout; not normally made publicly available

COMPUTER LAW & SECURITY REVIEW XXX (XXXX) XXX

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation ☆

Dimitra Markopoulou [a], *Vagelis Papakonstantinou* [a,*], *Paul de Hert* [a,b,†]

[a] *Vrije Universiteit Brussel (LSTS), Belgium*
[b] *Tilburg University (TILT), the Netherlands*

ARTICLE INFO

Article history:
Available online xxx

Keywords:
EU data protection
Cybersecurity
NIS Directive
ENISA

ABSTRACT

The NIS Directive is the first horizontal legislation undertaken at EU level for the protection of network and information systems across the Union. During the last decades e-services, new technologies, information systems and networks have become embedded in our daily lives. It is by now common knowledge that deliberate incidents causing disruption of IT services and critical infrastructures constitute a serious threat to their operation and consequently to the functioning of the Internal Market and the Union. This paper first discusses the Directive's addressees particularly with regard to their compliance obligations as well as Member States' obligations as regards their respective national strategies and cooperation at EU level. Subsequently, the critical role of ENISA in implementing the Directive, as reinforced by the proposal for a new Regulation on ENISA (the EU Cybersecurity Act), is brought forward, before elaborating upon the, inevitable, relationship of the NIS Directive with EU's General Data Protection Regulation.

1. Introduction

Directive 2016/1148[1] on security of network and information systems (the NIS Directive) is the first horizontal legislation undertaken at European Union (EU) level for the protection of network and information systems across the Union. During the last decades e-services, new technologies, information systems and networks have become embedded in our daily lives. It is by now common knowledge that deliberate incidents causing disruption of IT services and critical infrastructures constitute a serious threat to their operation and

☆ This research has been funded under the European Commission's H2020 project FORTIKA – Cyber Security Accelerator for trusted SMEs IT Ecosystems, Grant Agreement 740690.

* Corresponding author: Vagelis Papakonstantinou, Vrije Universiteit Brussel (LSTS), Belgium.
E-mail addresses: dimitra.markopoulou@vub.be (D. Markopoulou), evangelos.papakonstantinou@vub.be (V. Papakonstantinou), paul.de.hert@vub.ac.be (P. de Hert).

† The authors wish to thank Lina Jasmontaite for useful comments and feedback.

[1] Directive 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive").

https://doi.org/10.1016/j.clsr.2019.06.007

consequently to the functioning of the Internal Market and the Union.[2] This risk, combined with the fact that existing counter-measures in terms of security tools and procedures are not sufficiently developed in the EU, and certainly not common in all Member States, made the need for a comprehensive approach at Union level, concerning the security of network and information systems, unquestionable. The NIS Directive aims to address this need by putting forward "*the measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market*".[3]

The NIS Directive was published in July 2016, however the EU has been addressing cyber security issues in a comprehensive manner since 2004, when ENISA (European Union Agency for Network and Information Security),[4] a new specialised EU agency, was founded. The NIS Directive itself has its roots in the Commission's Communication of 2009, which focuses on prevention and awareness and defines a plan of immediate action to strengthen the security and trust in the information society.[5] This was followed, in 2013, by a joint Communication released by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy on the Cybersecurity Strategy of the European Union.[6] From 2013 to 2015 the Commission, the Council and the Parliament discussed the draft put forward by the Commission intensely and these discussions resulted in the NIS Directive that entered into force in August 2016. The deadline for national transposition by the EU Member States was the 9th of May, 2018.[7,8]

The NIS Directive consists of 27 articles. Articles 1–6 set its scope and main definitions, including a further clarification regarding the identification of operators of essential services (article 5), as well as the meaning of significant disruptive effect (article 6). Articles 7–10 describe the national frameworks that need to be adopted by each Member State on the security of network and information systems. These frameworks include, among others, Member States' obligation to introduce a national strategy and to designate national competent authorities (including a single point of contract and the computer security incident response teams (CSIRTs), as well as, the creation of the Cooperation Group. The cooperation mechanism is provided in Chapter III and more specifically in articles 11–13. The articles that follow (14–18) define the security requirements and incident notification for operators of essential services and digital service providers, respectively. The adoption of standards and the process of voluntary notification are dealt with in articles 19 and 20. Finally articles 21–27 include the Directive's final provisions.

In terms of structure, this article is divided into seven chapters: the first three chapters discuss the Directive's affected parties and their obligations under its provisions, chapters four and five set Member States' obligations as regards national strategy, as well as cooperation at EU level, whereas the critical role of ENISA in implementing the Directive, as this is reinforced by the proposal for a new Regulation on ENISA (the EU Cybersecurity Act),[9] is presented in chapter 6. Finally, the, inevitable, relationship of the Directive with EU's General Data Protection Regulation[10] are established in the final chapter 7.

2. Operators of essential services (first target of the NIS Directive)

2.1. *Definition: an Annex approach*

The NIS Directive affects two categories of undertakings, under an admittedly differentiated approach in terms of obligations placed upon each one of them: operators of essential services and digital service providers.[11] Their definitions are included in article 4 and consist of a combination of articles of this Directive[12] and its annexes, as well as Directive (EU) 2015/1535.[13] With regard to the first category, that is operators of essential services, their definition includes a public or private entity that activates in specific sectors, such as the sector of energy, transport, banking and health,[14] and which at the same time meets some essential criteria that qualify it as an entity of such type.[15] Consequently, not all operators of essential services fall within the scope of the NIS Directive. Member

[2] For cyber-crime statistics see Carrapico H./Farrand B. in *Cybercrime as a fragmented policy field in the context of the area of freedom, security and justice*, in Ripoll Servent A./Trauner F. (Eds.), Routledge Handbook on the Area of Freedom, Security and Justice, Routledge, 2018.

[3] See article 1 of the NIS Directive.

[4] See https://www.ENISA.europa.eu/.

[5] See Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience (COM (2009)149).

[6] Joint Communication to the European Parliament, the Council the European Economic and Social Committee and the Committee of the regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (available at http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf).

[7] See article 25 of the Directive (transposition).

[8] At the time of drafting this paper the majority of Member States have implemented the Directive.

[9] See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN.

[10] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[11] On identifying the entities under cyber security obligations see also Kulesza J. in *Defining Cybersecurity-Cybersecurity and Critical Infrastructure, the Actors*, in Kulesza J./Balleste R. (Eds.) *Cybersecurity and human rights in the age of cyberveilance*, Rowman & Littlefield, 2016.

[12] See article 4(2) on the definition of digital service and article 5(2) on the criteria an operator of essential services should meet.

[13] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

[14] For the full list of sectors and sub-sectors see Annex II of the NIS Directive and Section 1(a) of this paper.

[15] See article 5(2) of the NIS Directive: (a) an entity that provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident

Please cite this article as: Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007

States are tasked with the process of their categorisation and identification as such, as this is described in detail below.

In the event of sector specific Union legal acts, Member States should apply that legislation, as long as it contains requirements that are, at least, equivalent to the ones of the NIS Directive. Some examples include operators in the water transport sector,[16] undertakings providing public communication networks or publicly available communications services,[17] trust services providers,[18] as well as the sectors of banking and financial markets.[19]

We saw that operators of essential services include any private or public entity that meet specific criteria and at the same time are of the types included in Annex II of the NIS Directive. All entities that fall within this definition, should comply with the security and notification requirements included in the Directive. Annex II includes a list of the sectors and subsectors, as well as types of entities that are categorised as operators of essential services.[20] Once an entity is categorised as one of the types listed in the Annex, the next step lies with the Member States, who are responsible to carry out an identification process, in order to determine which individual companies meet the additional criteria of the definition of operators of essential services. To this end, the NIS Directive requires Member States to adopt national measures as a result of the identification process, in order to determine these entities.[21]

By 9 November 2018, Member States therefore had to identify the operators of essential services with an establishment on their territory for each sector and subsector referred to in the Annex.[22] This list of identified operators of essential services shall be updated by Member States at least every two years after May 9, 2018 in order to ensure that possible changes in the market are accurately reflected. Taking into account the minimum harmonisation requirement in article 3 of the Directive, Member States can adopt legislation ensuring a higher level of security. In this regard, Member States may expand the security and notification obligations provided for operators of essential services to entities belonging to other sectors and sub-sectors than those listed in the Annex of the NIS Directive. Accordingly, several additional sectors, not mentioned in the Annex, have been brought to the table by different Member States, including among others, public administrations, the postal sector, the food sector, the chemical and nuclear industry, the environmental sector and civil protection.[23]

2.2. *Security requirements (art. 14 par. 1 and 2 of the NIS Directive)*

Pursuant to article 14 (1) of the NIS Directive, Member States are required to ensure that operators of essential services take appropriate measures, technical and organisational, to manage the risks posed to the security of the network and information systems they use. In accordance with article 14 (2), appropriate measures shall prevent and minimise the impact of incidents affecting the security of their systems. Main objective should be to ensure continuity of such services. How could a common perspective by all Member States be achieved though, as far as these security requirements are concerned? It is well understood that the Directive sets the general obligation for Member States to adopt a national strategy on this subject, however the specific approach to the national transposition of article 14 (1) of the Directive rests with each Member State. In order however for the national provisions on security requirements to be aligned to the greatest extent possible, the Commission encourages Member States to follow the guidance document developed by the Cooperation Group.[24] In this document the Cooperation Group lays down

would have significant disruptive effects on the provision of that service.

[16] See recital 11 of the NIS Directive where it is clarified that Member States, when identifying operators in the water transport sector, should take into consideration international codes and guidelines developed by the Maritime Organisations, as well as article 1 (7) of the Directive.

[17] See Framework Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services and the security requirements provided therein.

[18] See Regulation 910/2014 on electronic identification and trust services for electronic transactions in the Internal market and repealing Directive 1999/93/EC and the security requirements provided therein.

[19] See recital 12 of the NIS Directive: "Regulation and supervision in the sectors of banking and financial market infrastructures is highly harmonised at Union level, through the use of primary and secondary Union law and standards developed together with the European supervisory authorities. Within the banking union, the application and the supervision of those requirements are ensured by the single supervisory mechanism. For Member States that are not part of the banking union, this is ensured by the relevant banking regulators of Member States. In other areas of financial sector regulation, the European System of Financial Supervision also ensures a high degree of commonality and convergence in supervisory practices. The European Securities Markets Authority also plays a direct supervision role for certain entities, namely credit-rating agencies and trade repositories".

[20] In particular the following sectors and subsectors are listed: energy (electricity, oil and gas), transport (air, rail, water and road), banking (credit institutions, financial market infrastructures (trading venues, central counterparties), health (healthcare providers, including hospitals and private clinics), water (drinking water supply and distribution), and digital infrastructure (internet exchange points, domain name system service providers, top level domain names registries).

[21] See also recital 25 of the NIS Directive that reads as follows: "as a result of the identification process, Member States should adopt national measures to determine which entities are subject to obligations regarding the security of network and information systems. This result could be achieved by adopting a list enumerating all operators of essential services or by adopting national measures including objective quantifiable criteria, such as the output of the operator or the number of users, which make it possible to determine which entities are subject to obligations regarding the security of network and information systems. The national measures, whether already existing or adopted in the context of this Directive, should include all legal measures, administrative measures and policies allowing for the identification of operators of essential services under this Directive".

[22] See article 5 par. 1 of the NIS Directive.

[23] See Communication from the Commission to the European Parliament and the Council -Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM (2017) 476.

[24] See Cooperation Group's Reference document on security measures for operators of essential services, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

Please cite this article as: Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007

some general principles that should be taken into consideration by all Member States during adopting security measures. These measures should be effective, tailored, compatible, proportionate, concrete, verifiable and inclusive.

2.3. *Notification requirements (art. 14 par. 3 and 4 of the NIS Directive)*

The security requirements that need to be adopted by the operators of essential services are accompanied by another obligation that of notifying the competent authorities of any incident that has an impact on the continuity of the (essential) services an operator provides. Pursuant to article 14(3), Member States have to ensure that operators of essential services notify "*any incident having a significant impact on the continuity of the essential services*". Consequently, operators of essential services should not notify any minor incidents but only serious incidents affecting the continuity of the essential service. Article 14 par. 4 provides a list of parameters that should be taken into account, when determining the significance of the impact of an incident, namely the number of users affected, the duration of the incident and the geographical spread with regard to the area affected by the incident. Again, consistency in the national approaches, as far as the notification process is concerned, is of the essence. As in the case of security requirements, the Cooperation Group has published a reference document on this issue.[25]

3. Digital service providers (second target of the NIS Directive)

3.1. *Definition: a catch all approach*

Digital service providers are the second category of entities that fall under the scope of the NIS Directive. Digital service providers include any legal person that provides a digital service[26] and more specifically an online market place, an online search engine, or a cloud computing service.[27] Their regulation, as far as security and notification requirements are concerned, is justified due to the fact that many businesses depend on these providers for the provision of their own services. Consequently, a disruption of the digital service could have an impact on key economic and societal activities in the Union.[28] It should be noted that, in comparison to the operators of essential services, the NIS Directive does not require Member States to identify digital service providers, warranting thus a catch-all approach.

Three types of digital service providers fall under the scope of the NIS Directive: online market place providers, online search engine providers and cloud computing service providers. An online marketplace denotes a digital service[29] that allows consumers and/or traders to conclude online services or service contracts with traders.[30] An online search engine is described as a digital service that allows users to perform searches of websites on the basis of a query on any subject.[31] Finally, cloud computing service means, a digital service that enables access to a scalable and elastic pool of shareable computing resources.[32]

3.2. *Security requirements (art. 16 par. 1 and 2 of the NIS Directive)*

The Directive describes, in its article 16, the security measures that digital service providers should take in order to mitigate the risks that threaten the security of the network and information systems they use for the provision of their service. The same article regulates the incident notification process digital

[25] See Reference document on Incident Notification for operators of essential services. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

[26] That is a service within the meaning of point (b) of article 1(1) of Directive (EU) 2015/1535, which is of a type listed in Annex III of the NIS Directive. Accordingly, Service means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) "at a distance" means that the service is provided without the parties being simultaneously present; (ii) "by electronic means" means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) "at the individual request of a recipient of services" means that the service is provided through the transmission of data on individual request.

[27] The three types of services were chosen to be regulated due to the increasing number of businesses that fundamentally rely on them for the provision of their own services.

[28] See recital 48 of the NIS Directive that reads as follows: "the security, continuity and reliability of the type of digital services referred to in this Directive are of the essence for the smooth functioning of many businesses. A disruption of such a digital service could prevent the provision of other services which rely on it and could thus have an impact on key economic and societal activities in the Union. Such digital services might therefore be of crucial importance for the smooth functioning of businesses that depend on them and, moreover, for the participation of such businesses in the internal market and cross-border trade across the Union. Those digital service providers that are subject to this Directive are those that are considered to offer digital services on which many businesses in the Union increasingly rely".

[29] For the definition of digital service see footnote 13 above.

[30] See article 4(17) and recital 15 of the NIS Directive, as well as ENISA's Incident notification for DSPs in the context of the NIS Directive. As per article 4(17) "online marketplace" means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of article 4(1) of Directive 2013/11/EU of the European Parliaments and of the Council to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace.

[31] See article 4(18) of the Directive and recital 16 of the NIS Directive. As per article 4(18) online search engine means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found.

[32] See article 4(19) and also recital 17 of the NIS Directive. As per article 4(19) cloud computing service means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

Please cite this article as: Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007

service providers should follow in order to comply with the provisions of the Directive.

Article 16 (1) lists the elements that need to be taken into account by a digital service provider when identifying and adopting security measures for its network, that is: (a) the security of the systems and facilities, (b) incident handling, (c) business continuity management, (d) monitoring, auditing and testing and (e) compliance with international standards. The Commission, by virtue of article 16(8) of the NIS Directive,[33] issued an Implementing Regulation[34] that specifies further these elements.[35] The need for an additional legislative measure that clarifies the provisions of the NIS Directive, as far as the obligations of digital service providers are concerned, was considered essential. The reason for that is that digital service providers, contrary to operators of essential services, are free to take technical and organisational measures they consider appropriate and proportionate to manage the risk posed to the security of their systems. To this end, the guidelines and clarifications provided by the Implementing Regulation contribute so that digital service providers in the Union adopt, to the greatest extent possible, a common approach when addressing this issue.

3.3. *Notification requirements (art. 16 par. 3 and 4 of the NIS Directive)*

Except for the security requirements mentioned above, in order for a digital service provider to safeguard the security of its network and information system, an incident notification procedure should be followed. The obligation of digital service providers to notify any incidents with a substantial impact on the provision of their service is regulated under article 16 par. 3 and 4. In this context, Member States shall ensure that digital service providers notify the competent authority or the CSIRT (see below) of any incident with a substantial impact on the provision of their service. Article 16 (4) mentions the parameters to be taken into account in order to determine whether the impact of an incident is substantial, namely (a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident; (d) the extent of the disruption of the functioning of the service; (e) the extent of the impact on economic and societal activities. These parameters are further specified in the Implementing Regulation.[36]

This softer regulation of digital service providers in terms of security and notification requirements is also evident in their obligation to notify an incident only in those cases where they have access to the information needed to assess the impact of such incident.[37] Furthermore, in the case of digital service providers, contrary to operators of essential services, the competent authorities take action, if necessary, through ex post supervisory measures when provided with evidence by the digital service provider itself or a user or another competent authority.[38]

4. Is the different approach towards digital service providers and operators of essential services well justified?

The Directive's lighter approach towards digital service providers, as far as the security and notification requirements are concerned, as well as their ex post supervision by the competent authorities, is evident throughout its text. In addition to the Directive's main articles, many of its recitals deal extensively with the issue. Other than recital 60 mentioned above, recital 49 points out that digital service providers should be free to take measures they consider appropriate to manage the risks posed to their systems.[39] In the same context, recital 57 acknowledges the differences between operators of essential services and digital service providers and suggests that Member States should not identify digital service providers and at the same time should pursue a different level of harmonisation in relation to those two groups of entities.[40]

The softer approach towards digital service providers is mainly based on the different nature of the infrastructures they use as well as of the services they provide. It is not with-

[33] The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in article 22(2) by 9 August 2017.

[34] Commission Implementing Regulation (EU) 2018/151, of 30 January 2018, laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

[35] See article 2 of the Implementing Regulation.

[36] See articles 3 and 4 of the Implementing Regulation.

[37] See article 16(4) of the NIS Directive.

[38] See recital 60 of the NIS Directive "Digital service providers should be subject to light-touch and reactive ex post supervisory activities justified by the nature of their services and operations. The competent authority concerned should therefore only take action when provided with evidence, for example by the digital service provider itself, by another competent authority, including a competent authority of another Member State, or by a user of the service, that a digital service provider is not complying with the requirements of this Directive, in particular following the occurrence of an incident. The competent authority should therefore have no general obligation to supervise digital service providers". See also article 17 of the Directive.

[39] See recital 49 of the NIS Directive "…the security requirements for digital service providers should be lighter. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems".

[40] See recital 49: "Given the fundamental differences between operators of essential services, in particular their direct link with physical infrastructure, and digital service providers, in particular their cross-border nature, this Directive should take a differentiated approach with respect to the level of harmonisation in relation to those two groups of entities. For operators of essential services, Member States should be able to identify the relevant operators and impose stricter requirements than those laid down in this Directive. Member States should not identify digital service providers, as this Directive should apply to all digital service providers within its scope".

Please cite this article as: Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007

out meaning that the term "essential" distinguishes the services provided by the operators of essential services – it is even included in their definition. Moreover, the distinction "in favour" of digital service providers has an extra benefit for them, as it leaves them with more freedom to conduct business, which is considered a key factor to their successful operation. This is also the conclusion reached by ENISA, which, in its 2017 incident notifications for DSPs in the context of the NIS Directive paper, observes that "*In this respect, the light-touch approach aims at avoiding overburdening the DSPs while not hampering the capacity of the EU to react to cybersecurity incidents in a swift and efficient manner*".[41]

Should however this lighter treatment ever retreats when special conditions occur? For instance, there are cases where operators of essential services rely on digital service providers to provide their services. This would be the case for example of a hospital (operator of essential services activated in the health sector) hosting its patient records in the cloud (digital service provider that provides cloud computing services). Should these cases of digital service providers be treated differently? The NIS Directive, with the exception of some cases of national security and maintenance of law and order, strongly discourages Member States from imposing any further security and notification requirements on digital service providers.[42] However, there are several references in the text that leave space for a different reading of the Directive. Recital 54 for instance mentions that "*where public administrations in Member States use services offered by digital service providers, in particular cloud computing services, they might wish to require from the providers of such services additional security measures beyond what digital service providers would normally offer in compliance with the requirements of this Directive. They should be able to do so by means of contractual obligations*". Relevant reference is made also in recital 56, "*this Directive should not preclude Member States from adopting national measures requiring public-sector bodies to ensure specific security requirements when they contract cloud computing services. Any such national measures should apply to the public-sector body concerned and not to the cloud computing service provider*". Both recitals depict the same concern, that is, how security obligations of digital service providers could be strengthened if special conditions apply. What the NIS Directive suggests is that, if there is a need for additional security measures, this should be implemented contractually between the parties and not by means of the Directive's provisions. At the same time any further national security measures should apply to the operators of essential services and not to digital service providers. Article 16(5) leads to the same conclusion by defining that the burden of notifying an incident to the competent authority, even in cases where the operator of essential services relies on a third part digital service provider for the provision of the service, stays with the operators of essential services.

5. National frameworks on the security of network and information systems: national strategies and national authorities (articles 7–10 of the NIS Directive)

Each Member State must adopt a national framework in order to succeed compliance with the provisions of the NIS Directive. The national framework includes the national strategy on the security of network and information systems and the designation of the authorities that shall be responsible for the monitoring the implementation of the NIS Directive. As far as the first parameter is concerned, Article 7 of the Directive sets the obligation of each Member State to adopt a national strategy on the security of network and information systems in order to achieve a high level of security of such networks. This national strategy must address a list of issues, as described in article 7(1), including, among others, a risk assessment plan, a governance framework to achieve the objectives of the national strategy, the identification of measures relating to preparedness, response and recovery etc. Member States may turn to ENISA for advice and assistance when developing their national strategies. As per article 7(3) Member States ought to communicate their national strategies to the Commission within three months from their adoption.

Articles 8, 9, 11 and 12 of the NIS Directive specify the authorities and other bodies that shall be tasked with the role of monitoring its application at national and EU level. Each Member State ought to designate one or more national competent authorities on the security of network and information systems. These shall monitor the application of the NIS Directive at national level. Each Member State shall also designate a national Single Point of Contact to liaise and ensure cross-border cooperation with other Member States. Designated competent authorities and single point of contact, as well as their tasks, should be notified to the Commission (article 8).

Whether national competent authorities will be qualified to carry out this task is a question that can only be answered in practice. Undoubtedly, given the technical nature of its provisions and the complexity of the procedures provided for under the Directive, monitoring of its application by the competent authorities shall require expertise and profound technical knowledge. For now it suffices to say that the Directive, in its article 8 par. 5, sets Member States' obligation to ensure that the competent authorities and the single points of contact shall have adequate technical, financial and human resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. In practice, it is anticipated that both the Cooperation Group and ENISA shall, based on their technical expertise, prove useful assistants to this task. At the same time the European Commission has proposed a Regulation for the creation of a European Cybersecurity Industrial, Technology and Research competence Centre in an effort to invest in stronger and pioneering cybersecurity capacity in the EU. Once

[41] See https://www.ENISA.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive

[42] See article 16(10) "Without prejudice to article 1(6) member States shall not impose any further security or notification requirements on digital service providers." Article 1(6) reads as follows: "This Directive is without prejudice to the actions taken by Member States to safeguard their essential state functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences".

Please cite this article as: Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007

established, the Competence Centre shall also contribute to better understanding cybersecurity and reducing skills gaps on the Union related to cybersecurity.[43]

Member States are also asked to introduce one or more computer security incident response teams CSIRTs (article 9). The CSIRTs role, as per Annex I of the Directive, is to monitor incidents at national level, provide early warning, alerts and information to relevant stakeholders about risks and incidents, respond to incidents, provide dynamic risk and incident analysis and increase situational awareness, as well as, to participate in a network of the CSIRTs across Europe.

The NIS Directive does not impose a structure or hierarchy for the competent authority, the single point of contact or the CSIRTs. They may form a single organisation or be separate. Therefore, a CSIRT may be established within a competent authority. CSIRTs shall be responsible for risk and incident handling. As regards the relevant mechanism, all incident notifications received by the competent Authority or the CSIRTs shall be notified to the Single Point of Contact, which, in turn, shall submit annual summary reports to the Cooperation Group on the notifications received and the actions taken in accordance to the Directive.

The Directive's structure grants Member States space to design and adopt their national strategies on the security of network and information systems. The Directive sets the framework within which Member States should act as far as security and notification requirements for both operators of essential services and digital services providers are concerned. What these particular measures and requirements will be though rests entirely with each Member State. In view of the flexibility provided to Member States under the Directive, the first question that comes to mind is whether harmonised implementation of the Directive's provisions in different Member States is feasible.

Given that this is the first regulatory attempt at EU level for the protection of information systems and in view of the fact that the Directive aims to regulate a sector under constant reform and development, it is the authors' belief that this flexibility in implementation could prove beneficial in the long term. Allowing Member States to adapt the Directive's provisions to the needs and special characteristics of the undertakings operating within their territory could contribute to more effective assessment and implementation of the measures and requirements suggested in the Directive's text.

However, potentially diverging Member States' approaches is taken under consideration in the Directive's text. To this end a series of safeguards are introduced. More specifically, article 19 par. 1 of the Directive suggests that Member States encourage the use of European or internationally accepted standards and specifications in order to promote convergent implementation. At the same time both the Commission's Implementing Regulation,[44] as well as the Cooperation Group's guidance notes[45] are aimed towards the above purpose. ENISA's role while assisting Member States in implementing the Directive is also expected to contribute to the same end.[46] It remains to be seen, however, whether the above safeguards will suffice towards a harmonised implementation of the Directive within the EU.

6. Cooperation at EU level: the Cooperation Group (article 11), the CSIRTs network (article 12) and the Wannacry case

At EU level, the Cooperation Group ("CG") established under the NIS Directive (article 11), shall be chaired by the Presidency of the Council of the European Union. It shall gather representatives of Member States, the Commission (acting as secretariat) and ENISA. Given the importance of international cooperation on cybersecurity, the Group's role is to facilitate strategic cooperation and exchange of information among Member States and help develop trust and confidence. The Cooperation Group has met seven times to-date starting from February 2017.[47] The Group's tasks are described in article 11(3). Its functioning is further clarified by the Implementing Decision issued by the Commission, by virtue of article 11(5) of the Directive.[48,49]

Finally, article 12 establishes the creation of a network of the national CSIRT's. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU (the Computer Emergency Response Team for the EU institutions, agencies and bodies). Among the tasks that fall within the CSIRTs network's competencies is the exchange of information on CSIRTs' services, operations and cooperation capabilities, the exchange of information related to incidents and associated risks, identification of a coordinated response to an incident, and provision of support to Member States in addressing cross–border incidents. The Commission participates in the CSIRTs Network as an observer. ENISA provides secretariat services, actively supporting the cooperation among the CSIRTs. Two years after entry into force of the NIS Directive (by 9 August 2018), and every 18 months thereafter, the CSIRTs Network will produce a report assessing the benefits of operational cooperation, including conclusions and recommendations. The report will be sent to the Commission as a contribution to the review of the functioning of the Directive.

[43] See Proposal for a Regulation of the European parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, COM (2018) 630 final.
[44] See footnote 35.
[45] See footnotes 25 and 26.
[46] See Section 6 below: the role of ENISA in the new landscape.
[47] https://ec.europa.eu/digital-single-market/en/news/nis-cooperation-group-meetings-agendas
[48] Commission implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union
[49] Among others, the decision mentions that the Cooperation Group operates by consensus and can set up sub-groups to examine specific questions related to its work. The group works on the basis of biennial work programmes. Its main tasks are to steer the work of the Member States in the implementation of the Directive, by providing guidance to the CSIRTs network and assisting Member States in capacity building, sharing information and best practices on key issues, such as risks, incidents and cyber awareness.

Please cite this article as: Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007

The first recorded cyber security incident at EU level dates back to May 2017 and refers to the WannaCry Ransomware attack. The term ransomware[50] has been around for decades but the WannaCry attack was the first global ransomware heist that impacted entire state hospital systems, international businesses and countries as a whole. Estimates of that time suggested that approximately 190,000 computers in over 150 countries were affected.[51] This was a year in which the operational cooperation of the CSIRTs network was tested and proved its readiness and ability to cooperate during large scale security incidents. Despite its negative impact worldwide, this incident demonstrated the severity of large-scale cross border cyberattacks and triggered the need for international cooperation.[52]

7. The role of ENISA in the new landscape

ENISA is the European Union Agency for Network and Information Security. It is located in Greece (Heraclion Crete) and has an operational office in Athens. ENISA was founded by Regulation (EC) No 460/2004,[53] whereas its current regulatory framework consists of Regulation (EU) No 526/2013.[54] Since 2004, ENISA has been actively contributing towards warranting a high level of network and information security within the EU. ENISA's mission is to raise "*awareness of network and information security and to develop and promote a culture of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union*".[55] A proposal for a new Regulation on ENISA, repealing Regulation (EU) 526/2013 and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"),[56] promises to reform the Agency and enhance its capabilities and capacities aiming at achieving cybersecurity resilience and better supporting Member States. In December 2018, the European Commission, the European Parliament and the Council of the European Union reached a political agreement on the Cybersecurity Act.[57] In March 2019 the European Parliament adopted the Cybersecurity Act.[58] The Council of the European Union must now approve the Act resulting in this new EU Regulation that will enter into force 20 days after its publication in the EU Official Journal.

A broad description of ENISA's contribution to network and information security includes, among others, issuing recommendations, supporting policy-making, as well as "hands-on" work, whereby ENISA collaborates directly with operational teams throughout the EU. A summary of ENISA's strategy for the years 2016–2020 is being published,[59] incorporating the following priorities: (a) anticipate and support Europe in facing emerging network and information security challenges, (b) promote network and information security as an EU policy priority, (c) support Europe in maintaining state of the art NIS capacities, (d) foster the emerging European NIS Community, and (e) reinforce ENISA's impact.[60] At the same time ENISA actively assists the competent authorities by appointing its representative in the Cooperation Group and by providing the secretariat in the CSIRTs network.[61]

As regards the NIS Directive in particular, ENISA's role in implementing its provisions is practically embedded in its text. Recital 36 states that ENISA should assist Member States and the Commission by providing expertise whereas both Member States and the Commission should be able to consult ENISA.[62] Also, recital 38 refers to ENISA's responsibility to assist the Cooperation Group and be involved in the development of guidelines.[63] Finally, according to recital 69 the Commission should consult ENISA when adopting implementing acts.[64] ENISA's enhanced role is also evident in several of the Directive's articles.[65]

In practice, and as far as digital service providers are concerned, ENISA has issued a report to assist Member States in their effort to provide a common approach regarding the minimum security measures for digital service providers.[66] Objectives of the report are to define common baseline security objectives for digital service providers, to describe different levels of sophistication in the implementation of security objectives, as well as to map the security objectives

[50] A virus infiltrates a computer device, locks down its data and would not release it until a ransom is paid.
[51] See https://www.ENISA.europa.eu/publications/info-notes/wannacry-ransomware-outburst
[52] See also https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ regarding the NotPetya attack.
[53] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), as amended by Regulation (EC) No 1007/2008 and amended by Regulation (EC) No 580/2011.
[54] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.
[55] See article 1 of ENISA's Regulation (EU) 526/2013.
[56] See footnote 10.
[57] See https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en
[58] See https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity
[59] See https://www.ENISA.europa.eu/publications/corporate/ENISA-strategy
[60] On the role of ENISA see also Robinson N. in *European Cyber Security policy*, in Andreasson K. (Ed.) *Cybersecurity, Public Sector Threat and Responses*, Taylor & Francis Group, 2012.
[61] See article 11 par. 2 and 12 par. 2 of the NIS Directive, respectively.
[62] See recital 36 "ENISA should assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practice. In particular, in the application of this Directive, the Commission should, and Member States should be able to, consult ENISA.
[63] See recital 38 "In general, ENISA should assist the Cooperation Group in the execution of its tasks…ENISA should also be involved in the development of guidelines for sector-specific criteria for determining the significance of the impact of an incident".
[64] See recital 69 "When adopting implementing acts on the security requirements for digital service providers, the Commission should take the utmost account of the opinion of ENISA".
[65] See for instance article 5 par. 7, article 7 par. 2, article 9 par. 5, article 12, article 19.
[66] See https://www.ENISA.europa.eu/publications/minimum-security-measures-for-digital-service-providers

Please cite this article as: Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007

against well-known industry standards, national frameworks and certification schemes.

In addition, ENISA has published another set of guidelines to further describe the incident notification process imposed on digital service providers as per article 16 of the NIS Directive.[67] Their objective, as stated in their par. 1.1, is "*to develop a set of guidelines for all concerned stakeholders (EU level authorities, public, private), aimed at supporting the implementation of the NIS Directive (hereafter referred to as "the Directive" or "NISD") requirements regarding mandatory incident notification*". The guidelines significantly contribute to further elaborating and clarifying notions that are included in the Directive's text, such as the "incidents" that fall within the notification obligation, the term "substantial impact" as well as the "parameters" that must be taken into account when determining the impact of an incident, as these are included in article 16(4) of the NIS Directive (number of users, duration of incident, geographical spread, extent of disruption and extent of impact on economic and societal activities).

The EU has already undertaken actions in order to enhance ENISA's role in ensuring a high level of network and information security, as well as in assisting Member States to implement an efficient national security policy for this purpose. Since its establishment in 2004, ENISA has been designated as a significant player in the cybersecurity industry. The NIS Directive further specified ENISA's powers and tasks and attributed to the Agency a key role as far as implementation of the Directive is concerned. An issue that remains unaddressed until today however, and which hopefully will be regulated by the new Regulation on ENISA,[68] is that ENISA remains the only EU agency with a fixed-term mandate. As pointed out in the Explanatory Memorandum of the Proposal for a Regulation on ENISA, this limits its ability to develop a long-term vision and support its stakeholders in a sustainable manner.

The fixed-term mandate also contrasts with the provisions of the Directive, which entrust ENISA with tasks with no end date. Under the Proposal, ENISA would be granted a permanent mandate and thus be put on a stable footing for the future.[69] This reform, in combination with the EU general ICT cybersecurity certification framework,[70] is considered as the preferred option in order for the EU to reach its objectives as far as its response to cybersecurity challenges is concerned.

In addition to the mandate amendment, the proposed regulation introduces some other novelties. In more detail it provides, among others, for an independent agency, that shall be named the "EU Cybersecurity Agency" and which shall operate as a centre of expertise on cybersecurity, shall assist the Union institutions, agencies and bodies, shall support capacity building and preparedness across the Union, shall promote cooperation across the Union and shall promote the use of certification by contributing to the establishment of a cybersecurity certification framework at Union level. In light of the continually evolving cyber threats and large-scale cross-border cybersecurity incidents, new enhanced role of ENISA's is urgently needed.

8. The NIS Directive and the General Data Protection Regulation

The General Data Protection Regulation, that became applicable on 25 May 2018, is aimed at protecting individuals with regard to the processing of their personal data, as well as, warranting the free movement of such data within the EU.[71] Release of the two legal instruments, the NIS Directive and the GDPR, largely coincided, the NIS Directive being published on July 2016 and the GDPR in April of the same year. However, the two law-making processes took place independently and in parallel, without much attention being paid from one to the other. Their only interaction was noted as early as in June 2013, in the form of an opinion issued by the EDPS on the NIS Directive.[72]

Neither the NIS Directive nor the GDPR acknowledges each other in their respective texts.[73] The NIS Directive only takes passing, if not limited, interest in data protection, in its article 2 or, for example, when mentioning that it "*respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, […]*",[74] or, by asking that competent authorities and DPAs cooperate whenever personal data are compromised in the event of incidents.[75] From its part, the GDPR takes account of cybersecurity-related processing only for its own aims and purposes, for example when clarifying that "*processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security constitutes a legitimate interest of the data controller concerned*", also listing CERTs and CSIRTs among recipients of these clarifications.[76]

In the same context, that of examining the relationship between the NIS Directive and the EU data protection system, some relevance may be found between the NIS Directive and the ePrivacy legal framework.[77] Notwithstanding the fact that the ePrivacy legal framework is sometimes broader than that of the GDPR, because privacy and confidentiality of

[67] See https://www.ENISA.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive

[68] See the Proposal for a Regulation as cited in recital 51 above.

[69] See the explanatory memorandum of the Proposal for a Regulation on ENISA at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN.

[70] The draft Proposal also outlines a cybersecurity certification scheme and the creation of the EU cybersecurity certification group (Articles 43-54 of the Proposal).

[71] See article 1 of the GDPR.

[72] See Preamble par. 73 of the NIS Directive.

[73] Admittedly, the NIS Directive does refer to the Data Protection Directive (Directive 95/46) that the GDPR replaced, in its Article 2, in however a passing, already outdated (the GDPR was already published) and mostly uninterested manner: "*processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC*".

[74] See Preamble, par. 75.

[75] See article 15.4 and par. 63 of the Preamble.

[76] See Preamble 49.

[77] As set, today, by the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, as amended and in effect today).

Please cite this article as: Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007

communications are explicitly listed within its scope, the definition of "*network and information systems*" in the NIS Directive explicitly includes "*electronic communications networks*" in the ePrivacy context,[78] thus invoking parallel application of the two legal instruments in relevant occasions. This in turn creates legal difficulties, not only because the ePrivacy EU legal framework is currently under review that will not become final in the near future,[79] but also because the relationship between the ePrivacy legal framework and the GDPR itself is at times problematic.[80]

Nevertheless, lack of explicit acknowledgement does not mean that the NIS Directive and the GDPR are unrelated.[81] On the contrary, as long as network and information systems are used for the processing of personal data, both legal instruments find application at the same time. It is therefore important first to identify points of interaction and then to discuss what happens in the event of conflicts.

As regards the former, points of interaction between the GDPR and the NIS Directive may occur whenever personal data are found in the systems of digital service providers and/or operators of essential services. An obvious first such point refers to the security of (personal) information. The principle of security of the personal data is one of the basic principles of the GDPR. While a relevant analysis exceeds the purposes of this paper, here it is enough to be noted that, according to the principle of integrity and confidentiality, "*personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*".[82] This is made concrete for controllers and processors in various provisions of the GDPR, most notably in a specialised article, article 32, but also while keeping records of their processing activities (Art. 30), while notifying data breaches (Art. 33), while preparing their impact assessments (Art. 35) or codes of conduct (Art. 40), or even when assessing the adequacy of the level of protection in a third country in international transfers (Art. 45).

The obvious question in this case is whether security measures undertaken in the context of the NIS Directive should be considered sufficient in the context of the GDPR, and vice versa. However, although this may be an expected and reasonable question on behalf of controllers and processors, or digital service providers and operators of essential services respectively, who would presumably wish to organise their compliance requirements as efficiently as possible, we consider it difficult for it to be answered *in abstracto*. Compliance obligations under each legal instrument are to be assessed separately, for different purposes, under different contexts, and indeed by different authorities. There is no apparent legal reason for decisions reached under one context to be considered binding under the other. Administrative fines or other enforcement measures, for the same purposes, should be considered cumulative and not mutually exclusive. Regardless of the fact that the practical network security measures may be the same for both legal instruments, we consider it essential that they be listed separately, in each compliance documentation respectively, and, in the event of a breach or incident, that they be judged independently, each for its own merits under the given circumstances and applicable legal framework.

Another point of interaction between the EU data protection and the EU cybersecurity legal systems could refer to an information systems' breach that would invite both an incident notification under the NIS Directive[83] and a data breach notification under the GDPR.[84] Could the two co-incide, or would a provider have to duplicate its effort so as to satisfy both legal instruments separately?[85] Here too the authors believe that an answer cannot be provided *in abstracto*, but would have to take into account the particular breach circumstances each time. In principle, however, again the two procedures should be considered unrelated and given the different subject-matter of the GDPR and the NIS Directive respectively, providers will most likely have to notify separately, each time under the requirements of each legal act.

As regards any cases of conflict between the NIS Directive and the GDPR, while in principle any scope overlaps ought to be resolved through a *lex specialis/lex generalis* relationship,[86] in the event of conflict, the GDPR will have to prevail. This is the result of both the GDPR implementing article 16(2) TFEU[87] as well as the presumed relationship between the applicable legal instruments each time. As regards the former, Article 16(2) TFEU added the right to data protection to the list of fundamental EU rights;[88] Consequently, respect of the right to data protection, as particularised in the text of the GDPR, constitutes a horizontal legal obligation within the EU and if these two obligations, meaning protection of personal data and cybersecurity, ever need to be balanced, the former will have to prevail.[89] This finding is further strengthened if the nature

[78] See article 4.1(a) of the Directive.

[79] Currently, the ePrivacy Regulation (COM 2017/10/final) is found at the *trilogue* EU law-making stage, most likely to be finalised in early 2019, which in turn means that a period of a few years until it becomes fully effective in the EU.

[80] The general idea being that the ePrivacy legal framework "complements and particularises" the GDPR, without this avoiding that cases of ambiguity altogether. See also European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities (12 March 2019).

[81] See also Kuner C/Svantesson D/Cate F/Lynskey O/Millard C in *The rise of cybersecurity and its impact on data protection*, editorial, International Data Privacy Law, Volume 7, Issue 2, 1 May 2017.

[82] See article 5.1(f) of the GDPR.

[83] See its Article 14.

[84] See its Article 33.

[85] On this issue see the UK ICO's guidance on "The GDPR and NIS" (https://ico.org.uk/for-organisations/the-guide-to-nis/gdpr-and-nis/) and also ENISA's "Incident notification for DSPs in the context of the NIS Directive", February 2017, p.20.

[86] Perhaps also in the spirit of article 2 of the NIS Directive.

[87] See also Preamble par. (1) and (12) of the GDPR.

[88] In its par. 1.

[89] See in particular the Breyer decision (CJEU, *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, par. 63 and 64), whereby the processing of personal data for security purposes (retention of the IP addresses of website visitors long after they had concluded their visit onto the respective websites) undertaken by internet site operators for prevention of security breaches (for example, "denial-of-service" attacks) was found to be falling under the

Please cite this article as: Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007

of potentially conflicting legal instruments is taken into consideration: The NIS Directive being implemented by national law at Member State level, a potential future conflict would therefore include an EU Regulation (the GDPR) against a Member State law, whereby the former would normally take precedence.[90]

When would any such conflict between the GDPR and the NIS Directive occur? For example, a Member State could decide to permit personal data processing operations otherwise prohibited or strictly regulated under the GDPR as part of its cybersecurity strategy, e.g. profiling on the basis of special categories of data (IP addresses coming from regions with high concentration of ethnic or religious populations) without the safeguards of article 22 of the GDPR. Or, an essential services provider could decide to store personal data for the purposes of cybersecurity for much longer than needed under the GDPR's principle of data minimisation.

Evidently, conflicting obligations are by no means expected to be the norm, and in fact the two legal instruments ought to be viewed rather as complementary, ultimately pursuing the same aim of (among others) strengthening the Internal Market.[91] In essence, obligations placed by the NIS Directive upon its recipients are expected to work to the benefit of individuals, whose personal data may be processed by the systems placed under its scope.

9. Conclusion

The NIS Directive could be considered a late response to an already exacerbated and well-known problem.[92] By now cybersecurity incidents, in the form of cyber-attacks and even cyber warfare have not only been identified at expert level but have also frequently captured public attention and press frontpages. An EU response, in the form of the NIS Directive, was long overdue in view of the many EU values at stake. However, the fact that a Directive allows Member States both space for flexibility and time for repose could be viewed as counter-productive, at least if EU's ultimate goal is the creation of an area of, indeed, cybersecurity.

Notwithstanding the choice of legal instrument, EU's response offers a well-thought of and balanced response that takes into account the (cybersecurity) problem and plans for the future. It establishes new, permanent, competent authorities at Member State level and introduces a system of cross-EU cooperation. National sensitivities and even budget restraints, as well as different levels of information technology sophistication, are also taken into account in the text of the NIS Directive, in the sense that it grants Member States room for manoeuvre (this time the choice of legal instrument playing in its favour rather than against it). OESs are evidently placed at the epicentre of attention, as was expected to be the case given their critical services. The DSPs that carry concrete compliance obligations under the NIS Directive are active today in these business sectors that, at least in contemporary business circumstances, are generally expected to have the financial means and human resources to successfully meet the challenge. ENISA's role is correctly strengthened – and is only expected to increase in importance in the future.

The NIS Directive's relationship with the GDPR, and the broader EU data protection edifice, has indeed attracted some attention and discussion, however we believe that this is mostly unwarranted. Each legal framework has its own aims and purposes and establishes its own mechanisms to achieve them. Their perspective also differs substantially: cybersecurity, unlike data protection, essentially does not grant any rights to individuals. Notwithstanding therefore the contemporary GDPR prevalence and ever-presence on all things digital, we believe that even on the few issues where the two legal frameworks intersect, one ought to leave the other largely unaffected, each security measure, personal data breach or incident being judged separately under its own circumstances.

Finally, it is important that one keeps the global perspective in mind. Cybersecurity is a critical field of global regulatory interest. China has introduced since 2017 its own cybersecurity law, which attracted various responses in the EU and elsewhere. The USA is implementing its own cybersecurity policy. The issue of data localisation,[93] that gravely affects any cybersecurity strategy, is being heatedly contested across the globe. The NIS Directive ought to be perceived as a single piece in a large, international, puzzle, perhaps the first EU piece in the game, hopefully soon to be followed, complemented and particularised by many others.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.clsr.2019.06.007.

"legitimate interests of the controller" legal basis, and was thus allowed by the Court, despite national (German) legislation prohibiting it. Consequently, in practice whenever personal data are being processed for (cyber)security purposes a balancing needs to be made, however at all times within the GDPR limits and boundaries. For example, while the mere retention of the IP addresses as above was deemed lawful by the Court under the "legitimate interests of the controller" legal basis, such conclusion ought not be taken for granted if more intrusive security-related processing was performed upon the same data (e.g. continuous on-line cross-examination against police databases in order to identify visits by known criminals). In other words, the balancing and assessment of the data protection and cybersecurity interests will always take place within GDPR and not NIS Directive grounds, giving thus precedence to the mechanism of the former.

[90] See also Preamble of the NIS Directive, par. 75.

[91] See Preamble par. 2 of the GDPR and Preamble par. 3 of the NIS Directive. See also Schünemann W/Baumann M-O (Eds.), Privacy, Data Protection and Cybersecurity in Europe, Springer, 2017.

[92] See also Carrapico H./Barrinha A. in *The EU as a Coherent (Cyber)Security Actor?, JCMS: Journal of Common Market Studies* 55, no. 6 (November 1, 2017): 1254–72, https://doi.org/10.1111/jcms.12575.

[93] See Kuner C in *Data nationalism and its discontents*, Emory Law Journal, Vol. 64 and also Bendiek A./Bossong R/Schulze M. in *The EU's Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges, SWP Comments* 47, November 2017.

Please cite this article as: Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007